Correcting Common VLAN Configuration Errors

BSMSN Module 2 Lesson 5

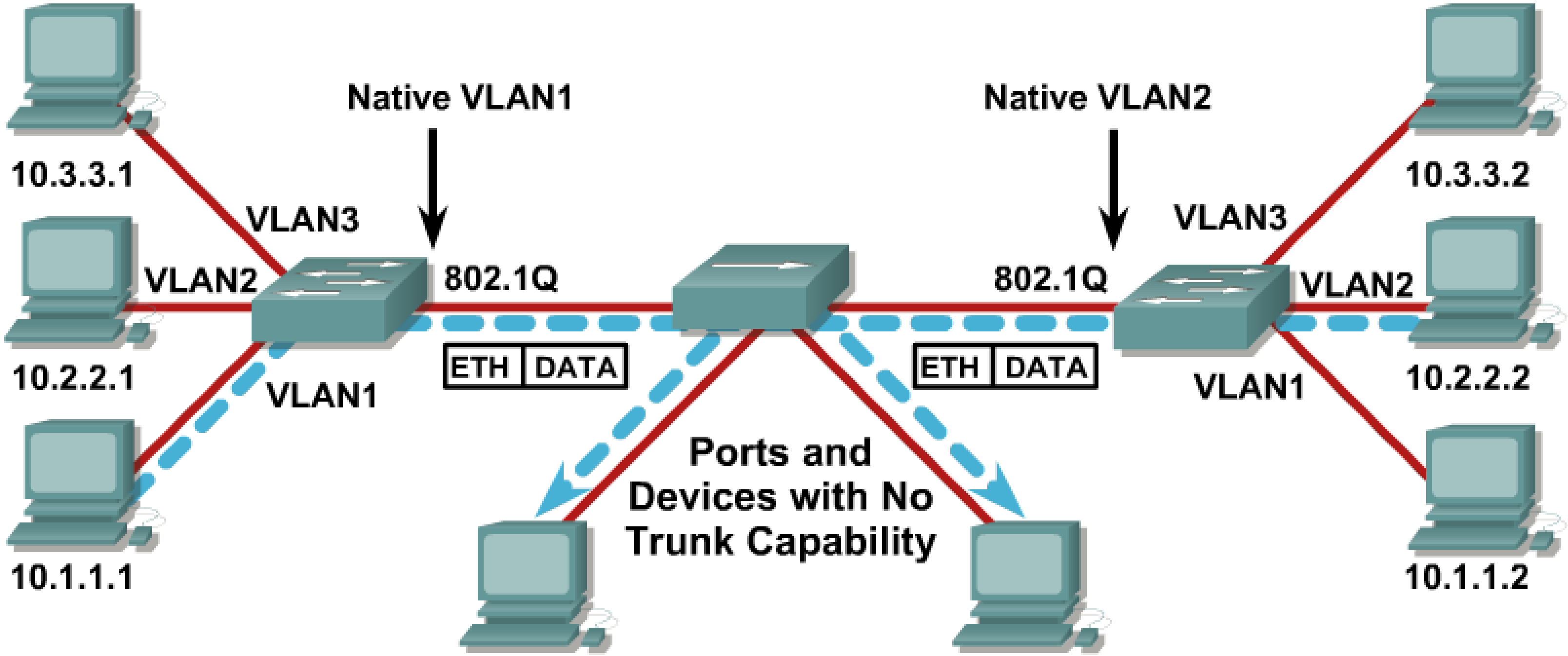
Objectives

- Describe issues with 802.1Q Native VLANs and explain how to resolve those issues.
- Describe trunk link problems and explain how to solve those.
- Identify common problems with VTP configuration.
- Describe best practices for using VTP in the Enterprise Composite Network Model.

Purpose of this Lesson

- What’s new in this module?
  - Description of issues with 802.1Q Native VLANs and how to resolve those issues.
  - Description of trunk link problems and how to solve those.
  - Common problems with VTP configuration.
  - Best practices for using VTP.
- This lesson does not cover VLANs. The VLAN modules of BCMSN are largely unchanged.

Different Native VLANs



A native VLAN mismatch will merge traffic between VLANs.

CDP and Unmatching Native VLANs

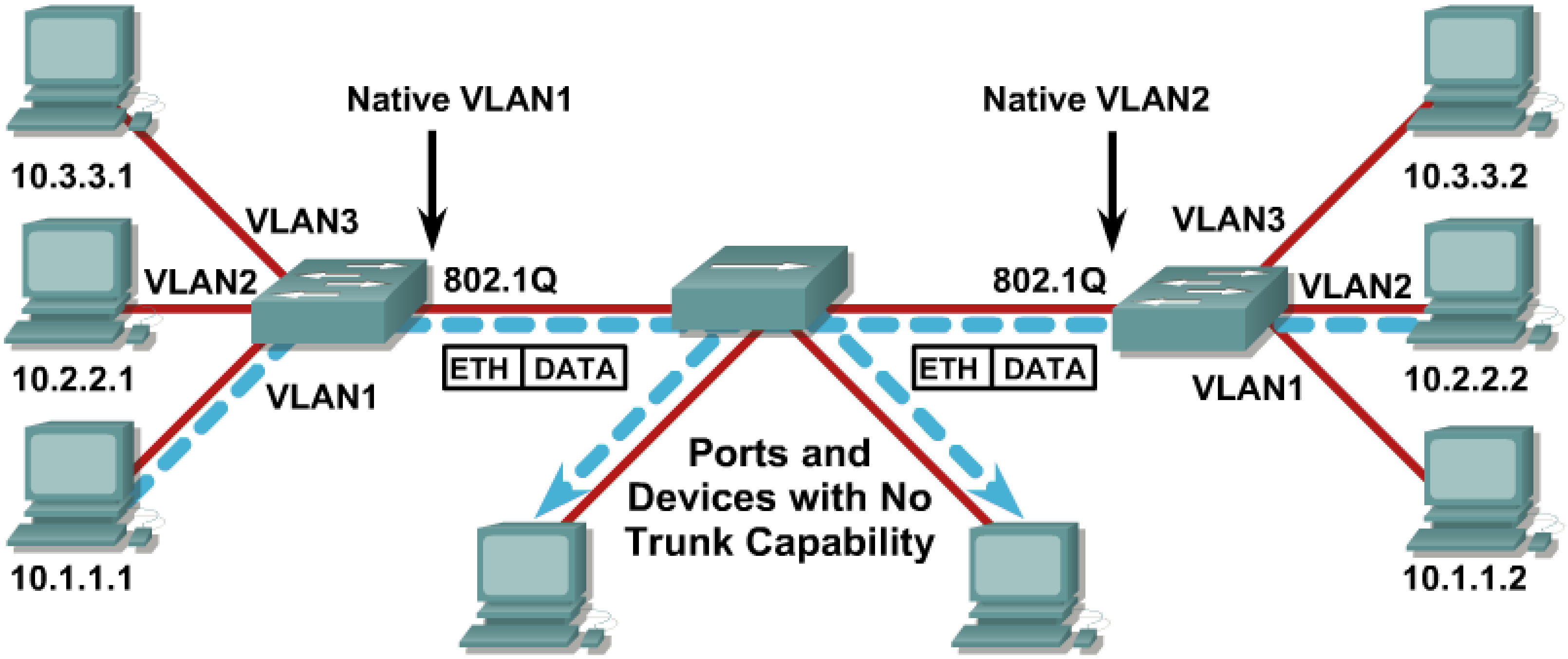
- Instances where unmatching VLAN IDs are reported between two devices are displayed in the console in the following format:

```
%NATIVE_VLAN_MISMATCH: native VLAN mismatch
discovered on [local interface (local interface
VLAN ID),] with [neighbor name neighbor
interface (neighbor VLAN ID)]
```

- In this example, a mismatch is reported on Ethernet 1/0 with native VLAN 5 and router1 Ethernet 2/3 with native VLAN 27:

```
%NATIVE_VLAN_MISMATCH: native VLAN mismatch
discovered on Ethernet1/0 (5), with router1
Ethernet2/3 (27)
```

Untagged Frames

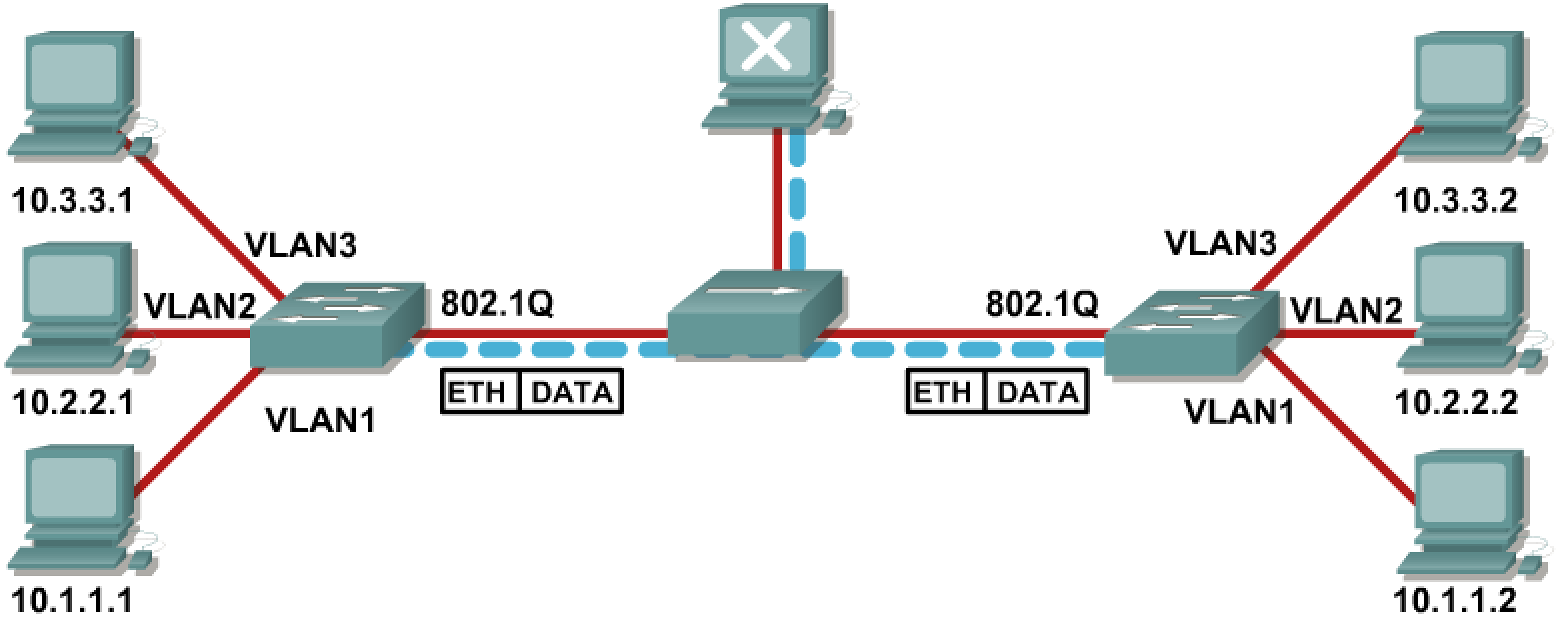


Native VLAN frames are carried over the trunk link untagged.

802.1Q Native VLAN Considerations

- Native VLAN must match at ends of trunk otherwise frames will ‘leak’ from one VLAN to another.
- By default the native VLAN will be VLAN1.

  Avoid using VLAN 1 for management purposes.
- Eliminate native VLANs from 802.1Q trunks by making the native VLAN an ‘unused’ VLAN.

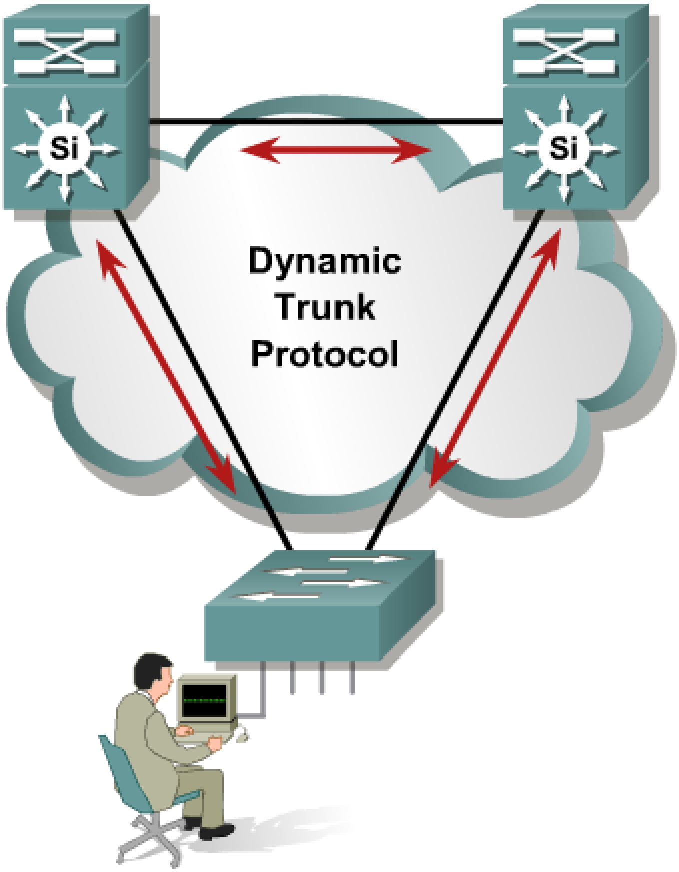


Explaining Trunk Link Problems

- Trunks can be configured statically or autonegotiated with DTP.
- For trunking to be autonegotiated, the switches must be in the same VTP domain.
- Some trunk configuration combinations will successfully configure a trunk, some will not.
- The following elements determine whether or not an operational trunk link is formed as well as the type of trunk the link becomes:
    - Trunking mode
    - Trunk encapsulation type
    - VLAN Trunk Protocol (VTP) domain
    - Hardware capabilities of two connected ports

Dynamic Trunk Protocol (DTP)

- What is DTP?
  - Automates ISL/802.1Q trunk configuration
  - Operates between switches
  - Does not operate on routers
  - Not supported on 2900XL or 3500XL
- DTP synchronizes the trunking mode on link ends (i.e., native VLAN mismatch, VLAN range mismatch, encapsulation, etc.)
- DTP states on ISL/dot1Q trunking port can be set to
  - “auto”
  - “on”
  - “off”
  - “desirable”
  - “non-negotiate”

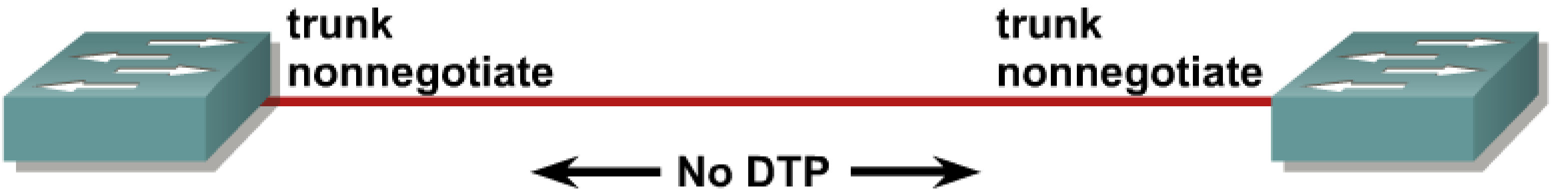


Trunk—Solution Trunking Modes

	Uses DTP	Forms Trunk with Off	Forms Trunk with Auto	Forms Trunk with Desirable	Forms Trunk with On	Forms Trunk with No Negotiate
Off	No	No	No	No	No	No
Auto	Yes	No	No	Yes	Yes	No
Desirable	Yes	No	Yes	Yes	Yes	No
On	Yes	No	Yes	Yes	Yes	Yes
No Negotiate	No	No	No	No	Yes	Yes

Resolving Trunk Link Problems

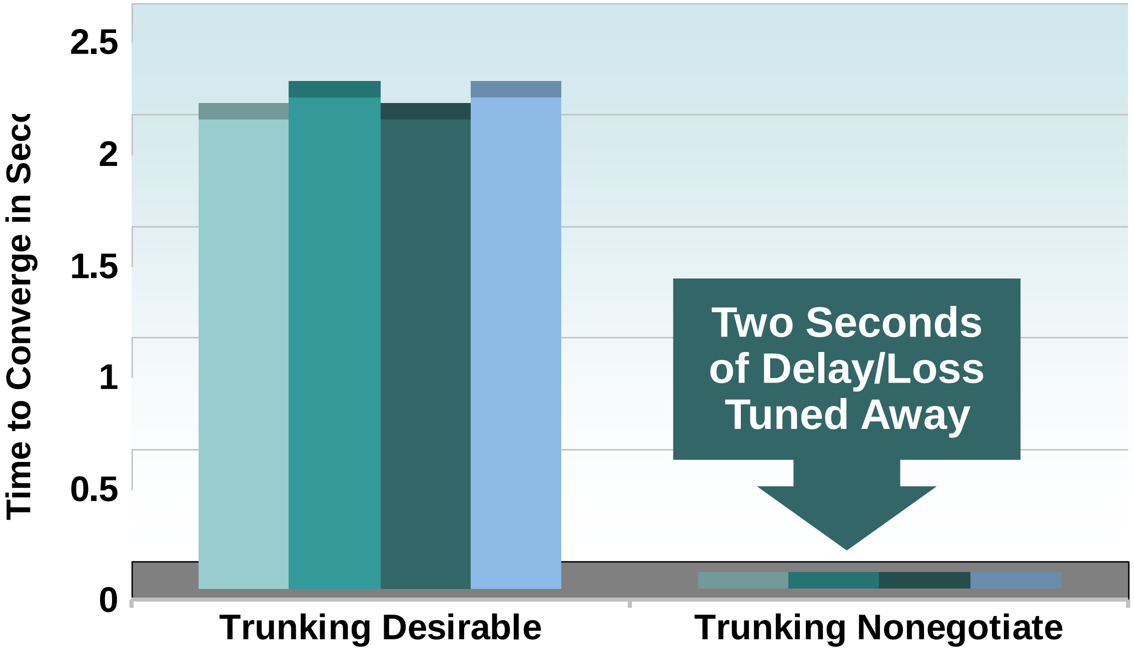
- When using DTP, ensure that both ends of the link are in the same VTP domain.
- Ensure that the trunk encapsulation type configured on both ends of the link is valid.
- DTP should be turned off on links where trunking is not required.
- Best practice is to configure **`trunk`** and **`nonegotiate`** where trunks are required.



Optimizing Convergence: Trunk Tuning
Trunk Auto/Desirable Takes Some Time

- DTP negotiation tuning improves link up convergence time

```
IOS(config-if)# switchport mode trunk
IOS(config-if)# switchport nonegotiate
```



Two Seconds of Delay/Loss Tuned Away

VTP Virtual Trunk Protocol

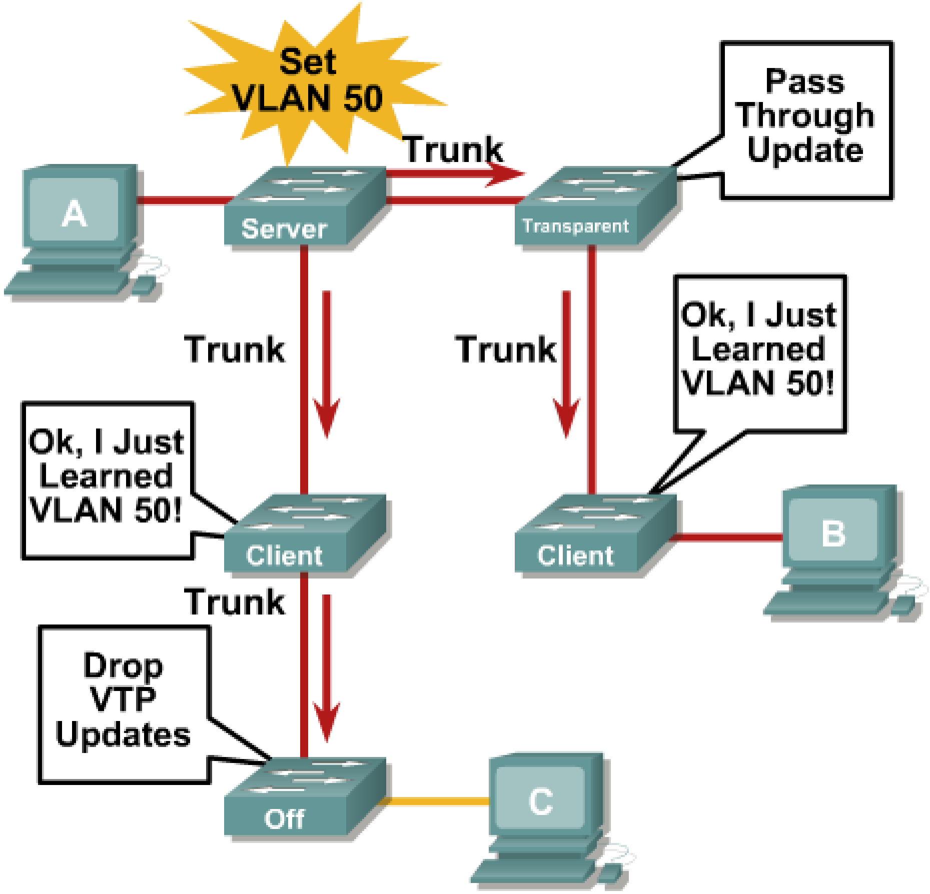
- Centralized VLAN management
- VTP server switch propagates VLAN database to VTP client switches
- Runs only on trunks
- Four modes:

  Server: updates clients and servers

  Client: receive updates—cannot make changes

  Transparent: let updates pass through

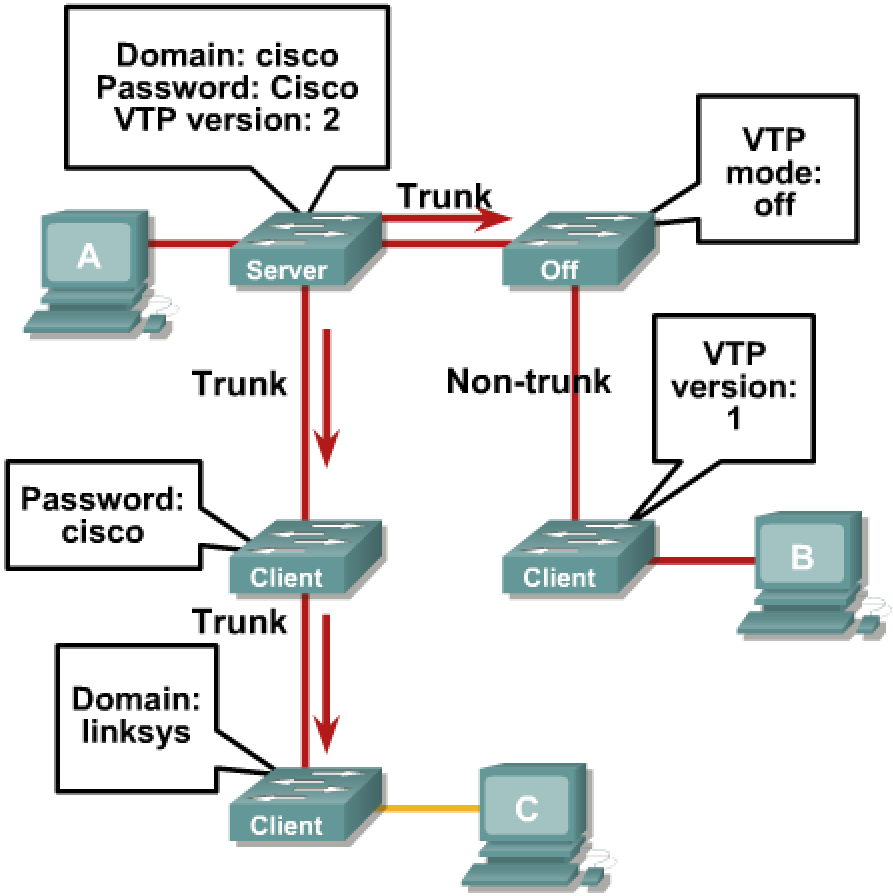
  Off: ignores VTP updates



Common Problems with VTP Configuration

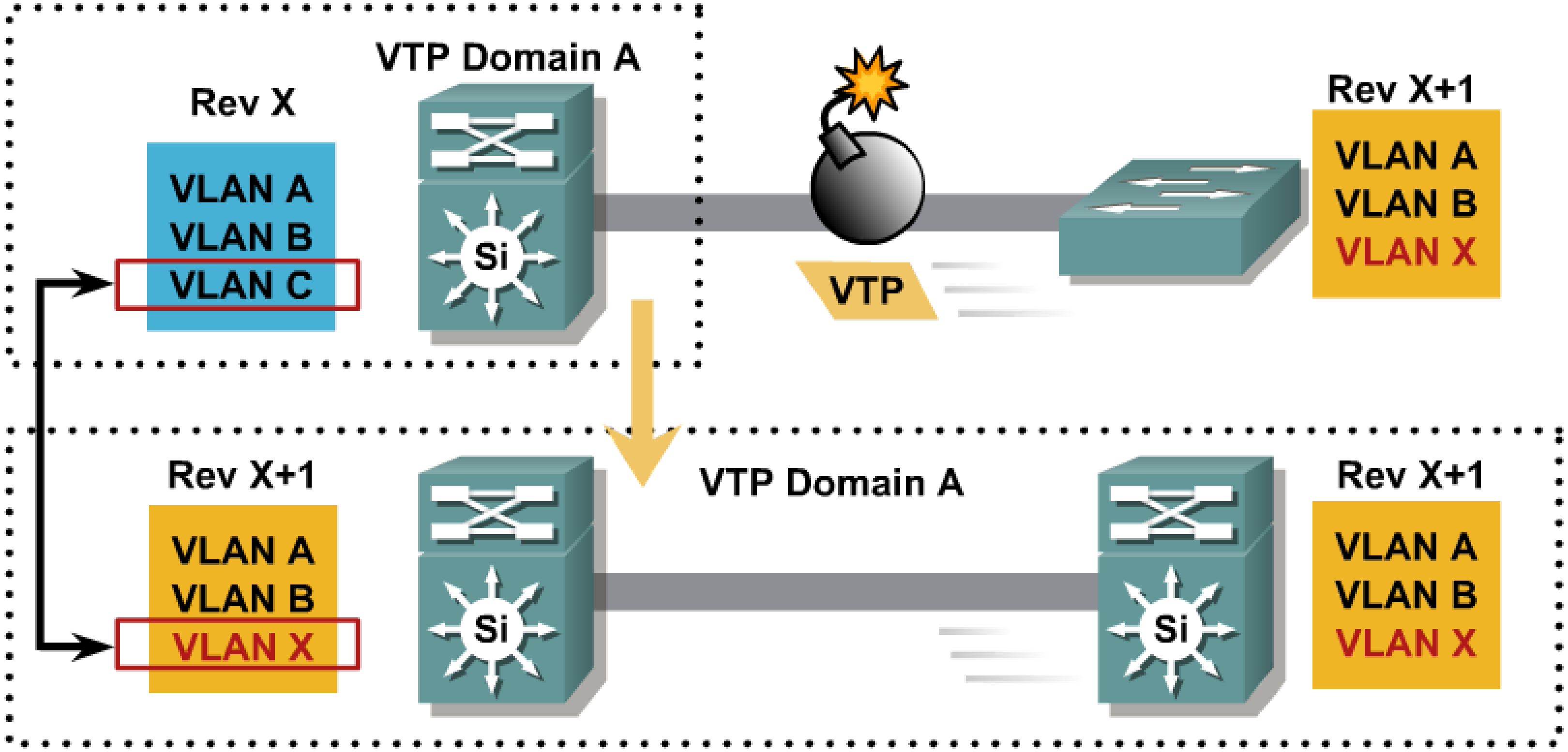
- Check domain name
- Check domain password
- Check VTP version
- Check trunk links
- Check VTP modes

  At least 1 server?



VLANs Disappear from Network

VTP Bomb occurs when a VTP Server with a Higher Revision of the VTP Database (Albeit Loaded with Potentially Incorrect Information) Is Inserted into the Production VTP Domain Causing the Loss of VLAN Information on All Switches in That VTP Domain



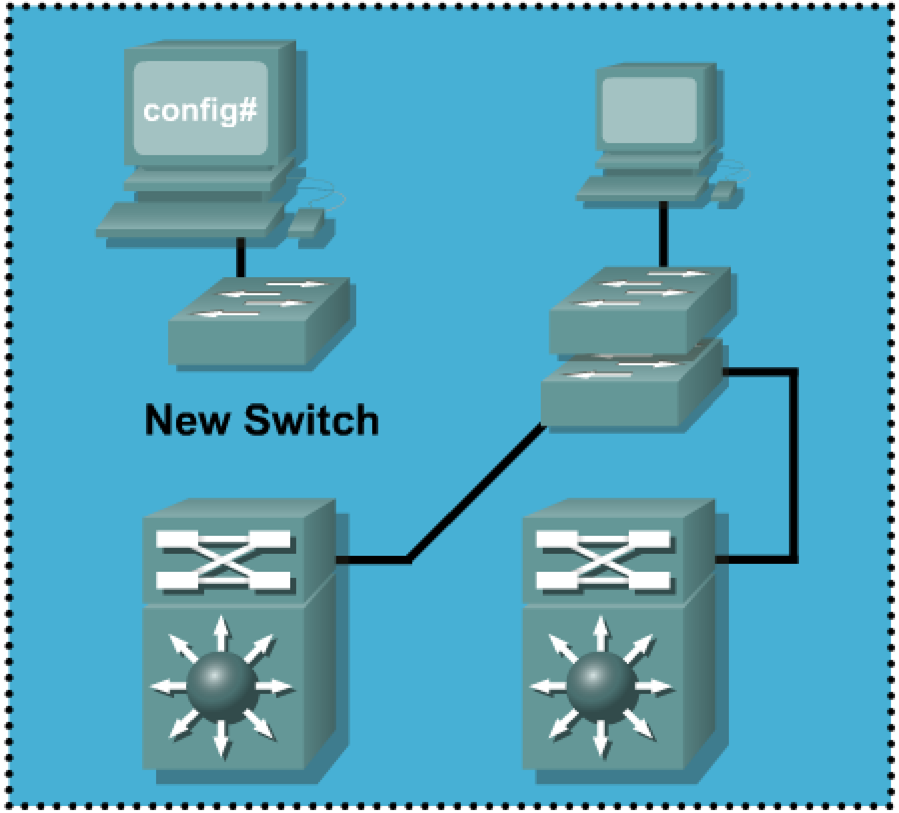
Example of New Switch Overwriting an Existing VTP Domain

New switch not connected:

```
Switch#show vtp status
VTP Version                    :2
Configuration Revision         :2
Number of existing VLANs       :7
VTP Operating Mode             :Server
VTP Domain Name                :building1
```

Existing switch:

```
Switch#show vtp status
VTP Version                    :2
Configuration Revision         :1
Number of existing VLANs       :6
VTP Operating Mode             :Server
VTP Domain Name                :building1
```

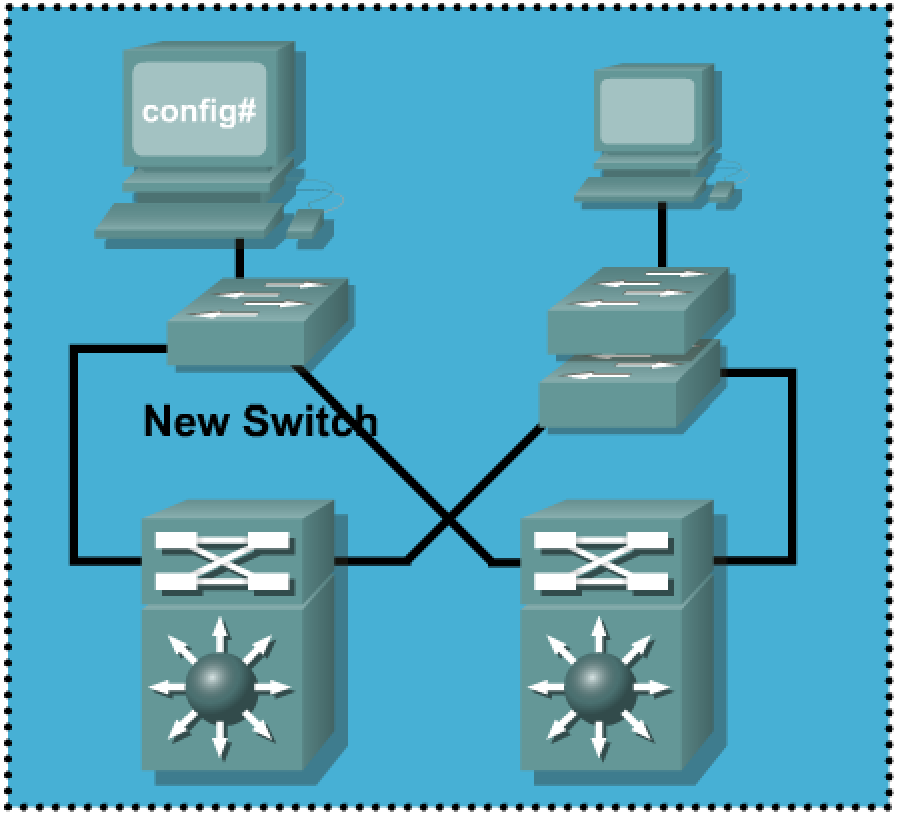


Example of New Switch Overwriting an Existing VTP Domain (cont.)

New switch after connection:

```
Switch#show vtp status
VTP Version                          :2
Configuration Revision               :2
Number of existing VLANs             :7
VTP Operating Mode                   :Server
VTP Domain Name                      :building1
```

New switch connected



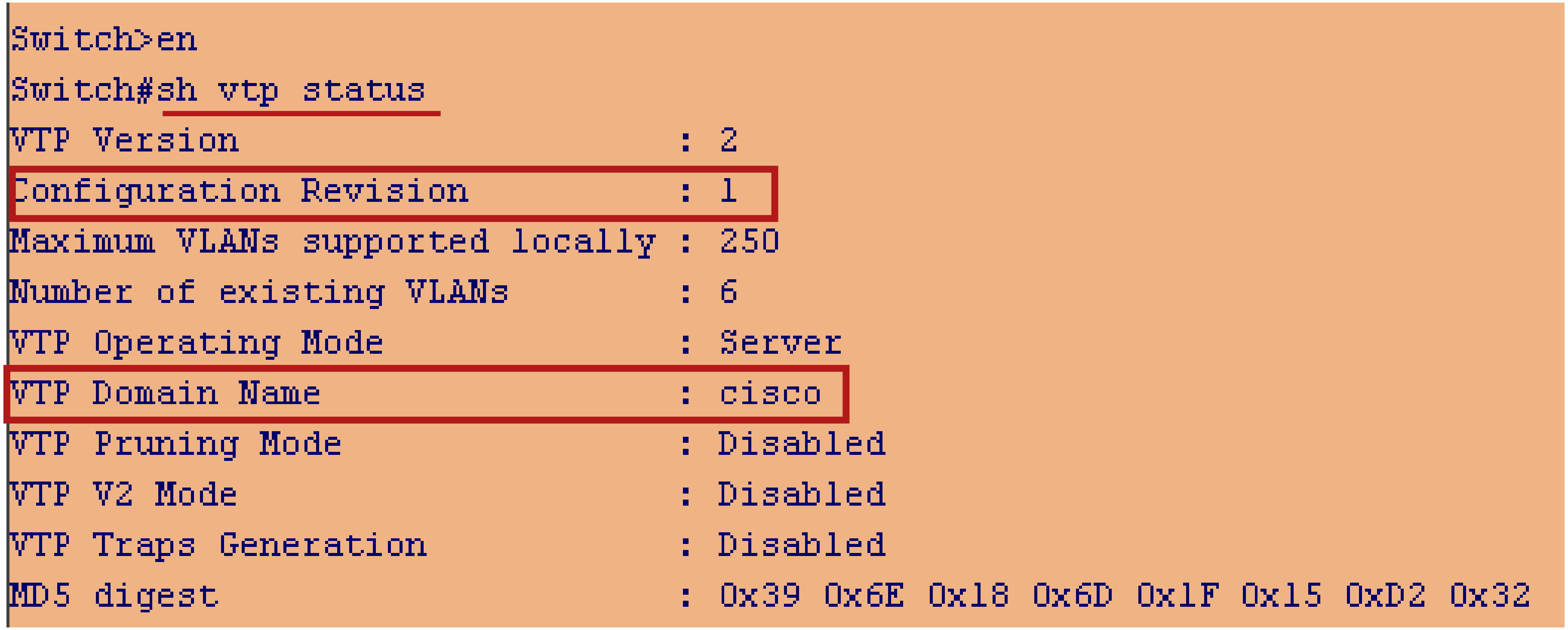
Existing switch after adding new:

```
Switch#show vtp status
VTP Version                          :2
Configuration Revision               :2
Number of existing VLANs             :7
VTP Operating Mode                   :Server
VTP Domain Name                      :building1
```

Resetting the VTP Revision Number

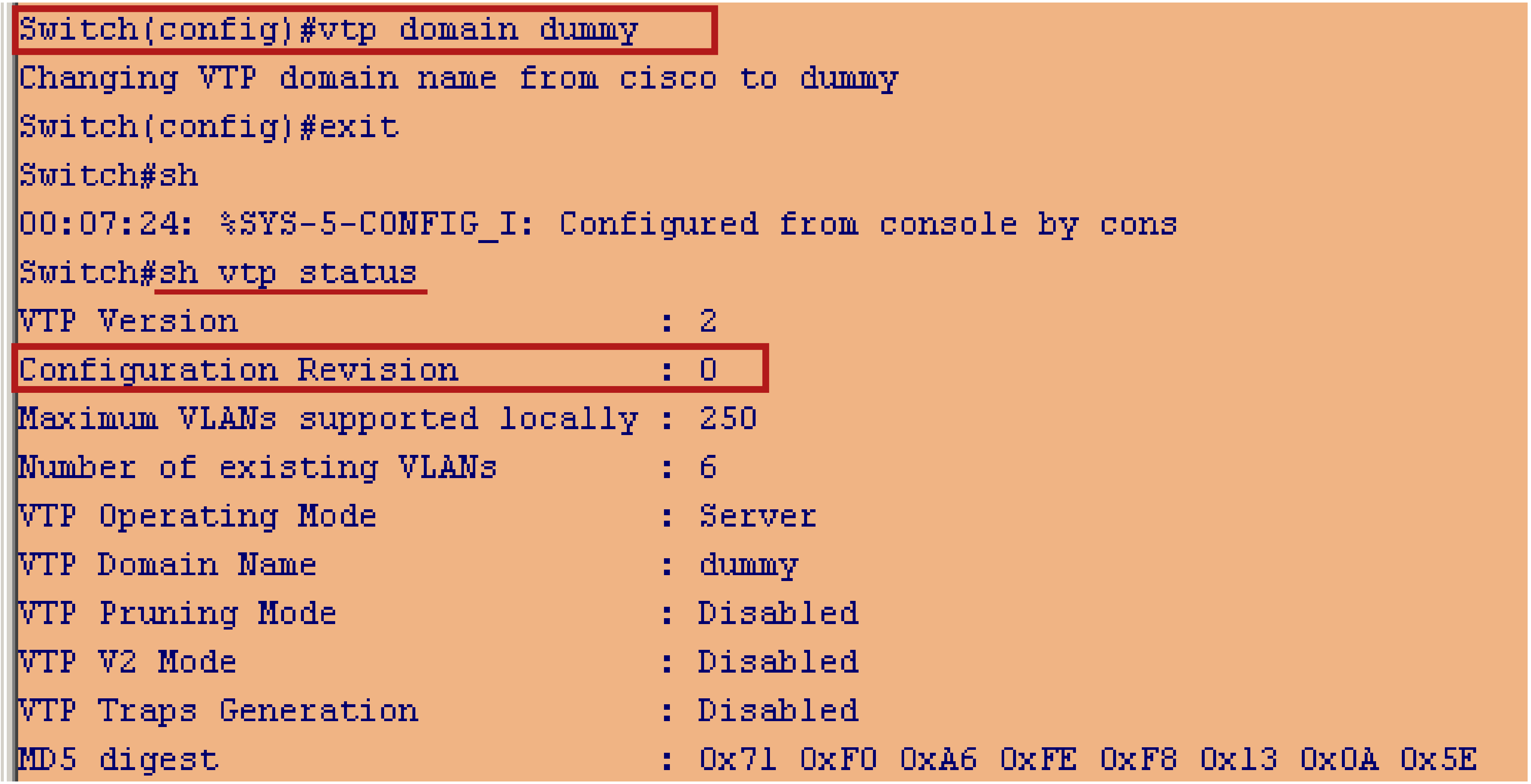
1. Use **show vtp status** command to check the VTP configuration revision number and the VTP domain name. If the revision number is 0, add the switch to the VTP domain. If the number is not 0, write down the domain name and proceed to Step 2.
2. Enter global configuration mode and use the **vtp domain *domain-name*** command to change the VTP domain name to something other than what was recorded in Step 1.
3. Issue the **end** command to exit configuration mode and save your changes
4. Use the **show vtp status** command to check the revision number. It should indicate 0.
5. Enter global configuration mode and use the **vtp domain *domain-name*** command to change the VTP domain name back to the name recorded in Step 1.
6. Issue the **end** command to exit configuration mode and save your changes
7. Use the **show vtp status** command to check the revision number. It should indicate 0.

Check Revision Number, Record Domain



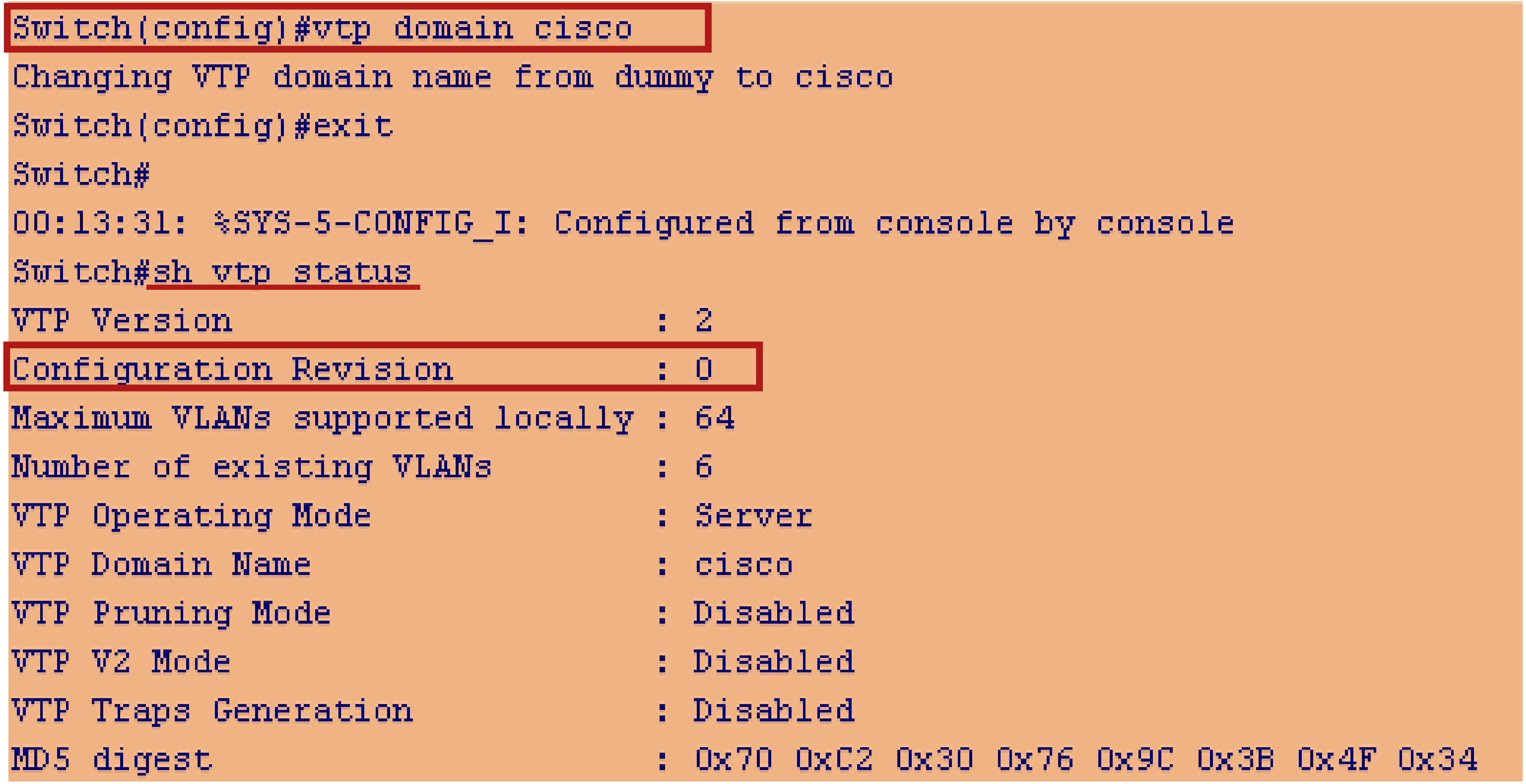
```
Switch>en
Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 250
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x39 0x6E 0x18 0x6D 0x1F 0x15 0xD2 0x32
```

Change Domain to Something New, Save Changes



```
Switch(config)#vtp domain dummy
Changing VTP domain name from cisco to dummy
Switch(config)#exit
Switch#sh
00:07:24: %SYS-5-CONFIG_I: Configured from console by cons
Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 250
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : dummy
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x71 0xF0 0xA6 0xFE 0xF8 0x13 0x0A 0x5E
```

Change Domain Back to Original and Confirm



```
Switch(config)#vtp domain cisco
Changing VTP domain name from dummy to cisco
Switch(config)#exit
Switch#
00:13:31: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x70 0xC2 0x30 0x76 0x9C 0x3B 0x4F 0x34
```

Implementing VTP in the Enterprise Composite Network Model

- Plan VTP domain boundaries.
- Have only one or two VTP servers.
- Configure a VTP password.
- Manually configure the VTP domain name on all devices.
- When setting up a new domain

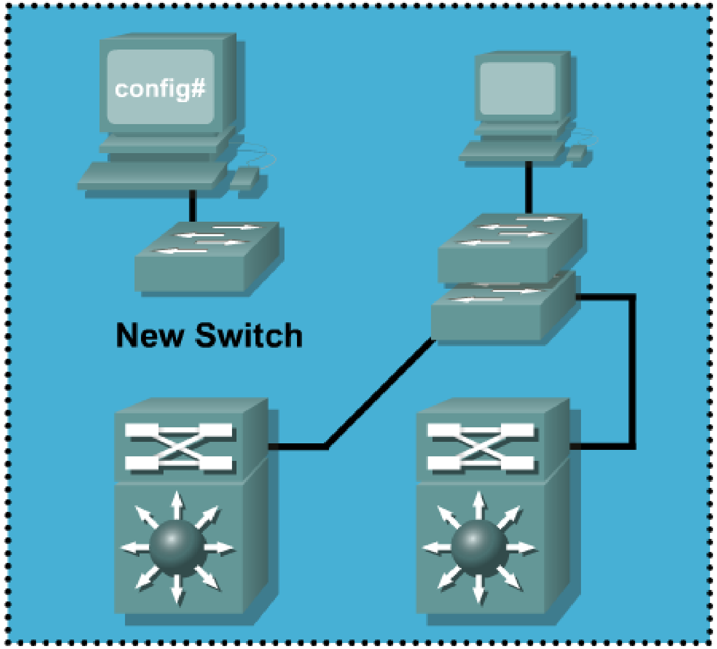
  Configure VTP client switches first so that they participate passively

- When cleaning up an existing VTP domain

  Configure passwords on servers first because clients may need to maintain current VLAN information until the server is verified as complete.

Activity

- You are tasked with adding a new switch to the existing network. The network is running VTP.
- Describe the steps you would take to ensure that the new switch did not overwrite the existing configuration.



Self Check

1. What is the danger of mismatched native VLANs?
2. What is the default native VLAN?
3. In a DTP configuration, what elements determine whether or not an operational trunk link is formed as well as the type of trunk the link becomes?
4. Name 4 VTP modes and describe their VTP roles.
5. What is a VTP Bomb?

Summary

- 802.1Q native VLAN can cause security issues.
- Configure the native VLAN to be an ‘unused’ VLAN.
- Some trunk link configuration combinations can result in problems on the link.
- Best practice is to configure trunks statically rather than with DTP.
- Misconfiguration of VTP can give unexpected results.
- Make only one or two VTP servers; keep the remainder as clients.

Resources

- DTP Messages:

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12111yj/2950smg/msg_desc.htm#xtocid3

- Cisco Command Reference:

  http://www.cisco.com/en/US/products/ ps6441/prod_command_reference_list.html

- TAC Case Collection (requires CCO login)

  http://www.ciscotaccc.com/lanswitching/home

Q and A